

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-200479

(43) 公開日 平成7年(1995)8月4日

(51) Int. Cl. <sup>6</sup>

G06F 15/00

識別記号

330

庁内整理番号

B 7459-5L

F I

技術表示箇所

審査請求 未請求 請求項の数 2 O L (全 8 頁)

(21) 出願番号 特願平5-334624

(22) 出願日 平成5年(1993)12月28日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(71) 出願人 000233055

日立ソフトウェアエンジニアリング株式会社

神奈川県横浜市中区尾上町6丁目81番地

(72) 発明者 畔原 謙一

神奈川県川崎市幸区鹿島田890番地の12

株式会社日立製作所情報システム事業部内

(74) 代理人 弁理士 小川 勝男

最終頁に続く

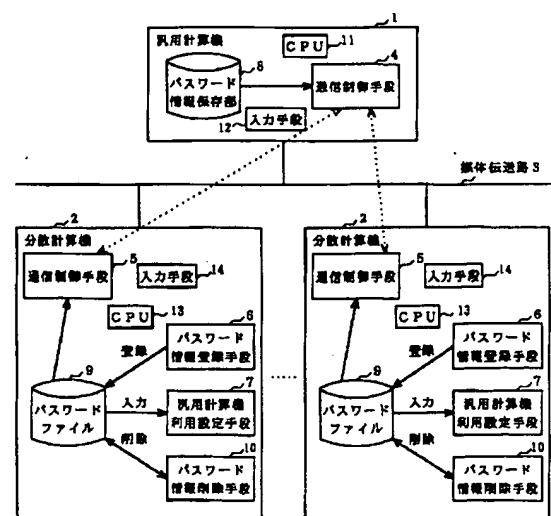
(54) 【発明の名称】 パスワード管理システム

(57) 【要約】

【目的】 分散システムにおいてホスト側での1回のパスワード情報登録操作だけでパスワード情報を効率良く分散機側でも管理できるようにする。

【構成】 分散計算機2の入力手段14から利用者IDが入力されると、該利用者IDに対応するパスワード情報をパスワードファイル9から読み込み、入力されたパスワードがパスワードファイル9のパスワードと一致すれば分散計算機2の利用を可能とし、パスワードファイル9に対応するパスワード情報が無ければ、利用者IDを汎用計算機1に送信し、パスワード情報保存部8内の該利用者IDに対応するパスワード情報を分散計算機2に送信し、パスワードファイル9に登録する。登録したパスワードと入力されたパスワードを比較し、一致すれば分散計算機2の利用を可能とする。

図1



## 【特許請求の範囲】

【請求項 1】ホスト計算機と分散計算機が伝送路によって接続され、パスワードによって分散計算機の利用を管理している分散システムにおいて、

ホスト計算機に、パスワードを利用者識別情報と関連づけて保存する記憶手段と、分散計算機から転送された利用者識別情報に基づいて該当するパスワード情報を前記記憶手段から読み込む制御手段と、分散計算機とパスワード情報の送受信を行う通信制御手段を設け、

分散計算機に、ホスト計算機から転送されたパスワード情報を登録する記憶手段と、利用者識別情報とパスワードを入力する入力手段と、前記ホスト計算機とパスワード情報の送受信を行う通信制御手段と、ホスト計算機から転送されたパスワード情報に日付情報を付加して記憶手段に登録する登録手段と、前記入力手段から入力された利用者識別情報に基づいて該当するパスワード情報を記憶手段から読み込み、該パスワードと入力手段から入力されたパスワードを比較して一致した場合に分散計算機の利用を可能とする制御手段を設けたことを特徴とするパスワード管理システム。

【請求項 2】前記分散計算機の記憶手段におけるパスワード情報の登録許可件数を前記分散計算機の入力手段で前記分散計算機の制御手段に予め設定しておき、前記分散計算機の書き込み手段が前記記憶手段に登録すると前記制御手段が登録件数と登録許可件数を比較し、登録件数が登録許可件数以上になると制御手段が日付情報が最も古いパスワード情報を指定して、指定されたパスワード情報を削除する削除手段を設けたことを特徴とする請求項 1 記載のパスワード管理システム。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】本発明は汎用計算機と分散計算機で構成されるシステムにおいて、利用者毎にシステム共通のパスワード情報を管理する方法に関するものである。

## 【0002】

【従来の技術】従来汎用計算機と分散計算機におけるパスワード情報の管理方式は、特開昭 63-104536 号公報に記載のように各ハンディターミナル利用のための共通のパスワード情報を CPU で一元管理し、入力された利用者コードに該当するパスワード情報をその都度各ハンディターミナルに転送することで、入力されたパスワードと照合することにより、汎用計算機の利用者を管理していた。

## 【0003】

【発明が解決しようとする課題】上記従来技術は、ハンディターミナルにパスワードを予め格納しておくことについて開示されておらず、パスワードをホスト側と端末側で 2 元管理する点については考慮されていなかった。また、この 2 元管理のときにパスワードのメインテナン

スをどのように行うかについては、全く考慮されていなかった。

【0004】本発明は、分散システムにおいて 1 回のパスワード情報登録操作だけで 2 元管理した利用者毎のパスワード情報を効率良く管理できるようにしたパスワード管理システムを提供することを目的とする。

## 【0005】

【課題を解決するための手段】汎用計算機等のホスト計算機には、分散計算機を利用するためのパスワード情報を一括して利用者識別情報ごとに予め保存しておく記憶手段と、分散計算機とパスワード情報の送受信をする通信制御手段と、汎用計算機の制御を行う CPU を設け、分散計算機には、利用者がパスワード情報を入力する入力手段と、汎用計算機とパスワード情報の送受信をする通信制御手段と、該分散計算機を利用した利用者の汎用計算機から受信したパスワード情報のみを利用者識別情報ごとに登録した記憶手段と、ホスト計算機から受信したパスワード情報を前記記憶手段に登録する登録手段と、分散計算機の制御を行う CPU を設けることにより、上記問題を解決する。

## 【0006】

【作用】汎用計算機側の記憶手段には登録手段により予め利用可能なパスワード情報を一括して登録しておく。分散計算機側で利用者により入力手段から利用者識別情報が入力されると、CPU が利用者識別情報をキーにしてパスワード情報を登録した分散計算機側の記憶手段を検索する。検索の結果、該当するパスワード情報が登録されていれば、該パスワード情報を CPU に読み込み、利用者識別情報の入力の後に利用者が入力手段から入力したパスワードと CPU に読み込んだパスワード情報のパスワードを CPU により比較して一致すれば、分散計算機の利用が可能となる。

【0007】前記検索の結果、該当するパスワード情報が登録されていなければ、入力された利用者識別情報を通信制御手段により汎用計算機側の通信制御手段に送信し、汎用計算機側は利用者識別情報を受信すると、CPU が利用者識別情報をキーにしてパスワード情報を登録した汎用計算機側の記憶手段を検索する。検索の結果、該当するパスワード情報が登録されていれば、該パスワード情報を分散計算機側に送信し、該パスワード情報を受信すると CPU の命令により登録手段が分散計算機側の記憶手段に該パスワード情報を登録する。CPU に読み込み、利用者識別情報の入力の後に利用者が入力手段から入力したパスワードと CPU に読み込んだパスワード情報のパスワードを CPU により比較して一致すれば、分散計算機の利用が可能となる。

## 【0008】

【実施例】図 1 は、本発明のシステム構成の一実施例を示す図である。ホスト計算機である汎用計算機 1 と、端末である分散計算機 2 はそれぞれ媒体伝送路 3 によって

接続されている。汎用計算機 1 には、分散計算機 2 とパスワード情報を送受信する通信制御手段 4 と、分散計算機 2 利用のためのパスワード情報を予め登録しておくパスワード情報保存部 8 と、分散計算機 2 から送信された利用者 ID に該当するパスワード情報を検索したり、汎用計算機 1 の制御を行う CPU 11 と、パスワード情報保存部 8 に登録するためにパスワード情報を入力する入力手段 12 を設ける。分散計算機 2 には、パスワード情報を送受信する通信制御手段 5 と、分散計算機 2 の利用許可を与えるパスワード情報を登録するパスワードファイル 9 と、汎用計算機 1 から送信されたパスワード情報に当日の日付を示す情報を付加してパスワードファイル 9 に登録するパスワード情報登録手段 6、分散計算機 2 から汎用計算機 1 を利用する場合に該利用者のパスワード情報を汎用計算機利用画面に設定する汎用計算機利用設定手段 7 と、パスワードファイル 9 の登録を許可する最大件数に達したときパスワードファイルから削除するパスワード情報削除手段 10 と、利用者 ID に該当するパスワード情報を検索したり、パスワードファイル 9 に登録されたパスワードと利用者が入力したパスワードを比較したり汎用計算機 1 の制御を行う CPU 13 と、利用者が利用者 ID やパスワードを入力するための入力手段 14 を備える。ここでパスワード情報削除手段 10 は例えばアクセスした日付が一番古いパスワード情報を削除する。

【0009】図 2 はパスワード情報のデータ構成の一実施例を示す図であり、利用者の識別コードである利用者 ID 22 と、該利用者の暗証番号であるパスワード 23 と、分散計算機を利用した最終日付である最終利用日 24 から構成する。

【0010】次に、本発明の動作を説明する。図 10 は本発明のパスワード情報を共通化するための処理の流れを示すフローチャートである。例えば、パスワード情報保存部 8 に図 3 に示すデータ内容のパスワード情報が保存され、また、パスワードファイル 9 に図 4 に示すデータ内容のパスワード情報が登録されていたとする。ここで「USERA」はユーザを識別する利用者 ID で「PWDA」はそのユーザのパスワードである。図 4 の日付はそのユーザがアクセスした最新の日付（最終利用日）である。まず、分散計算機 2 において、利用者が図 12 に示す利用者入力画面 41 で入力手段 14 により、利用者 ID 「USERC」が入力されると（ステップ 51）、該利用者 ID に該当するパスワードがパスワードファイル 9 中に登録されているか否かのチェックを行う（ステップ 52）。図 4 に示すパスワードファイル 9 中のパスワード情報に利用者 ID 「USERC」のパスワード情報が存在しないため、入力手段 5 は利用者 ID 「USERC」を汎用計算機 1 の通信制御手段 4 に転送する（ステップ 53）。通信制御手段 4 が利用者 ID 「USERC」を受信すると CPU 11 がこの利用者 I

D を取得し（ステップ 54）、「USERC」に該当するパスワード情報がパスワード情報保存部 8 に存在するか否かのチェックを行い（ステップ 55）、図 3 に示すようにパスワード情報保存部 8 に利用者 ID 「USERC」のパスワード情報が存在するため、該パスワード情報を分散計算機 2 の通信制御手段 5 に転送する（ステップ 56）。通信制御手段 5 が該パスワード情報を受信するとパスワード情報登録手段 6 が該パスワード情報を取得すると（ステップ 57）、CPU 13 がパスワードファイル 9 のパスワード情報の既登録件数とパスワード情報削除手段 10 で予め設定した登録許可件数を比較して既登録件数が登録許可件数以上になると（ステップ 58）、パスワードファイル 3 に登録されたパスワード情報のうち最終利用日 24 の日付が最も古いパスワード情報を CPU 13 が指定して、パスワード情報削除手段 10 が該パスワード情報を削除する（ステップ 62）。ステップ 58 の比較で既登録件数が登録許可件数未満の場合は該パスワード情報に CPU 13 によって管理している日時情報に基づいて当日の日付を示す最終利用日 24 を付加してパスワードファイル 9 に登録する（ステップ 59）。ここでは、図 5 に示すように利用者 ID 「USERC」、パスワード「PWDC」のパスワード情報に最終利用日「93.09.03」を付加して登録する。利用者 ID の入力の後、引き続き利用者が入力手段 5 によって入力されたパスワードを CPU 11 が取得し（ステップ 60）、CPU は取得したパスワードとステップ 56 で登録したパスワードを比較して一致すれば、分散計算機 2 を利用できるようになり、不一致ならば、利用できない（ステップ 61）。本実施例では、図 5 に示すデータ内容のパスワード情報が登録されていることになるので、ステップ 59 で取得したパスワードが「PWDC」であれば分散計算機 2 の利用が可能になる。

【0011】次に、汎用計算機 1 のパスワード情報保存部 8 に登録されているパスワード情報のパスワードを変更する場合にパスワード情報を共通化するための処理の流れを図 5 および図 6～9 を用いて説明する。図 6 に示すデータ内容のパスワード情報がパスワード情報保存部 8 に、また図 7 に示すデータ内容のパスワード情報がパスワードファイル 9 に登録されていたが、汎用計算機 1 側で管理者がパスワード情報保存部 8 の利用者 ID 「USERM」のパスワードを「PWDM」を「PWDZ」に変更した場合、パスワード情報保存部 8 のデータ内容は、図 8 で示すデータ内容になる。分散計算機 2 において、利用者により利用者 ID 「USERM」を入力されると（ステップ 51）、パスワードファイル 9 に該当する情報があるかどうかを CPU 13 が検索し（ステップ 52）、該当する情報がなければステップ 53～60 のパスワード情報を登録する処理に移り、該当する情報があるならば、次に CPU 13 は利用者により入力手段 14 から入力されたパスワードを取得する（ステップ 6

5

1)。ここでは、図7のデータ内容が示す通り、パスワードファイル9には利用者ID「USERM」が登録されているので、ステップ61に移り分散計算機2側で変更登録した後のパスワード「PWDZ」を利用者入力画面24で利用者によって入力手段14から入力されると、CPU13が「PWDZ」を取得する。次にステップ51で取得した利用者IDに該当するパスワードファイル9のパスワードとステップ61で取得したパスワードを比較し(ステップ62)、一致したならば分散計算機2の利用が可能となる。ここでは図7のデータ内容が示すようにパスワードファイル9の該当パスワードは「PWDM」であるため不一致となり、ステップ51で取得した利用者IDを通信制御手段5から汎用計算機1の通信制御手段4に転送し(ステップ63)、通信制御手段4が利用者IDを受信するとCPU11は該利用者IDを取得して、該利用者IDに該当するパスワード情報をパスワード情報保存部8から読み込んで(ステップ64)、該パスワード情報を通信制御手段4から分散計算機2の通信制御手段5に転送する(ステップ65)。ここでは、図8が示す通り該当するパスワード情報は利用者ID22が「USERM」でパスワード23が「PWDZ」のものであり、このパスワード情報が転送される。通信制御手段5が該パスワード情報を受信するとパスワード情報登録手段6が該パスワード情報を取得する(ステップ66)。パスワード情報登録手段6は該パスワード情報に当日の日付を示す情報を最終利用日24として付加してパスワードファイル9に登録する(ステップ67)。ここでは、図9で示すように「93.09.03」が最終利用日24として付加して登録される。そして、ステップ51で取得した利用者IDに該当するパスワードファイル9中のパスワードとステップ61で取得したパスワードをCPU11で比較し(ステップ68)、一致すれば分散計算機2の利用が可能となり、不一致ならば利用不可となる。ここでは、ステップ51で取得した利用者ID「USERM」に該当するパスワードファイル9中のパスワード「PWDZ」とステップ61で取得したパスワード「PWDZ」が一致するので利用可能となる。上記動作のように汎用計算機1のパスワード情報保存部8のパスワード情報のみを変更しておけば、利用する分散計算機2で変更後のパスワードを入力することによりパスワードファイル9のパスワード情報も変更される。

【0012】次に汎用計算機1と分散計算機2の間に、パスワード情報管理計算機75を設けた場合の第2の実施例を図11を用いて説明する。汎用計算機1にはパスワード情報を保存するマスタデータ保存部76と、マスタデータ保存部76で新たに登録又は変更されたパスワード情報をパスワード情報管理計算機75に転送する通信制御手段77と、汎用コンピュータ1の制御を行うCPU78を設ける。パスワード情報管理計算機75は図

6

1で示す汎用計算機1と同じハードウェア構成からなり、パスワード情報保存部8に登録されるデータ内容は、汎用計算機1のマスタデータ保存部76のデータ内容が反映されて更新される。汎用計算機1側で管理者等により入力手段79から新たにパスワード情報が登録又は更新されると、CPU78が新しいパスワード情報を通信制御手段77から送信するように制御する。パスワード情報管理計算機75は汎用計算機1の運用時と運用時以外にも運用しておき、汎用計算機1が運用している場合は、汎用計算機1とパスワード情報管理計算機75のどちらにも分散計算機2利用のためのパスワード情報の問い合わせをすることができ、たとえ汎用計算機1が運用していなくてもパスワード情報管理計算機75にパスワード情報の問い合わせをすることができるので、汎用計算機1が運用時間外であってもパスワード情報管理計算機75と分散計算機2が運用していれば、分散計算機2で入力された利用者IDに該当するパスワード情報抽出のための問い合わせが可能となる。

【0013】また、分散計算機2を汎用計算機1の端末として利用する場合には、利用者が分散計算機2の入力手段により汎用計算機利用設定手段7の起動を指示すると、利用者が入力した利用者IDを基にパスワードファイル9にある該当パスワード情報を抽出し、抽出した利用者IDとパスワードを汎用計算機1利用のパスワード情報として利用者入力画面に設定することにより、パスワードが一致すれば汎用計算機1の利用が可能となる。

【0014】図12は分散計算機2で利用者がパスワード情報を入力する際の利用者入力画面の一例であり、ディスプレイ画面41上にパスワード情報の入力項目として利用者ID42とパスワード43がある。

【0015】以上、本願発明の実施例について説明したが、本願発明はこれらの実施例に限られず、その趣旨を逸脱しない範囲で種々の変形が可能である。例えば、本実施例では汎用計算機側のパスワードを修正した後であっても分散計算機側では修正前及び修正後の両方のパスワードが利用可能となるが、これを防ぐために汎用計算機側のパスワードを変更した時は必ず分散計算機側にその利用者IDを通知してパスワードを更新したり、分散計算機側でその利用者IDのパスワード情報を削除するようにすれば良い。さらに汎用計算機側でパスワードの変更、削除を行った時には分散計算機側のパスワード情報を全て削除して初期化するようにしても良い。

【0016】

【発明の効果】本発明によれば、汎用計算機のパスワード情報保存部8の1回のパスワード情報の登録操作により、利用者毎にパスワード情報をシステム全体で共通化できるので、各分散計算機にパスワード情報を登録しなくても分散計算機の利用が可能となる。

【0017】また、汎用計算機1のパスワード情報保存

部8のパスワード情報のみを変更しておけば、変更されたパスワードを分散計算機2利用のために入力することによりパスワードファイル9のパスワード情報も変更される。

【0018】また、古い順にパスワード情報を随時削除することが可能であり、またパスワードファイル9の登録可能な件数を越えた場合による登録の失敗を防ぐことができる。

【図面の簡単な説明】

【図1】本発明のシステム構成の一実施例を示す図

【図2】パスワード情報のデータ構成の一実施例を示す図

【図3】パスワード情報保存部内のパスワード情報のデータ内容を示す図

【図4】パスワードファイル内のパスワード情報のデータ内容を示す図

【図5】パスワードファイル内のパスワード情報のデータ内容を示す図

【図6】パスワード情報保存部内のパスワード情報のデータ内容を示す図

【図7】パスワードファイル内のパスワード情報のデータ内容を示す図

【図8】パスワード情報保存部内のパスワード情報のデータ内容を示す図

ータ内容を示す図

【図9】パスワードファイル内のパスワード情報のデータ内容を示す図

【図10】本発明のパスワード情報を共通化するための処理手順を示す図

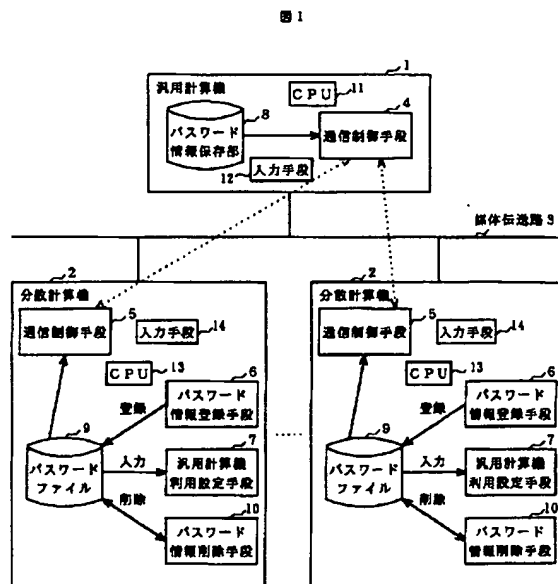
【図11】パスワード管理計算機を設けたシステム構成の一実施例を示す図

【図12】利用者入力画面の一実施例を示す図

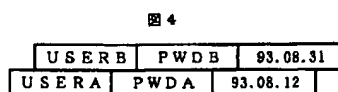
【符号の説明】

- 1 汎用計算機
- 2 分散計算機
- 3 媒体伝送路
- 4 通信制御手段
- 5 通信制御手段
- 6 パスワード情報登録手段
- 7 汎用計算機利用設定手段
- 8 パスワード情報保存部
- 9 パスワードファイル
- 10 パスワード情報削除手段
- 11 CPU
- 12 入力手段
- 13 CPU
- 14 入力手段

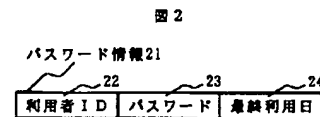
【図1】



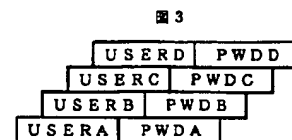
【図4】



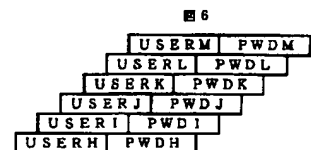
【図2】



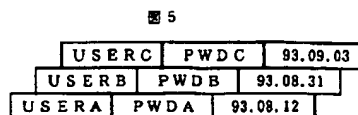
【図3】



【図6】



【図5】



【図 7】

図 7

USERM	PWDM	93.09.02
USERK	PWDK	93.09.02
USERJ	PWDJ	93.07.21
USERI	PWDI	93.08.29
USERH	PWDH	93.07.21

【図 8】

図 8

USERM	PWDZ
USERL	PWDL
USERK	PWDK
USERJ	PWDJ
USERI	PWDI
USERH	PWDH

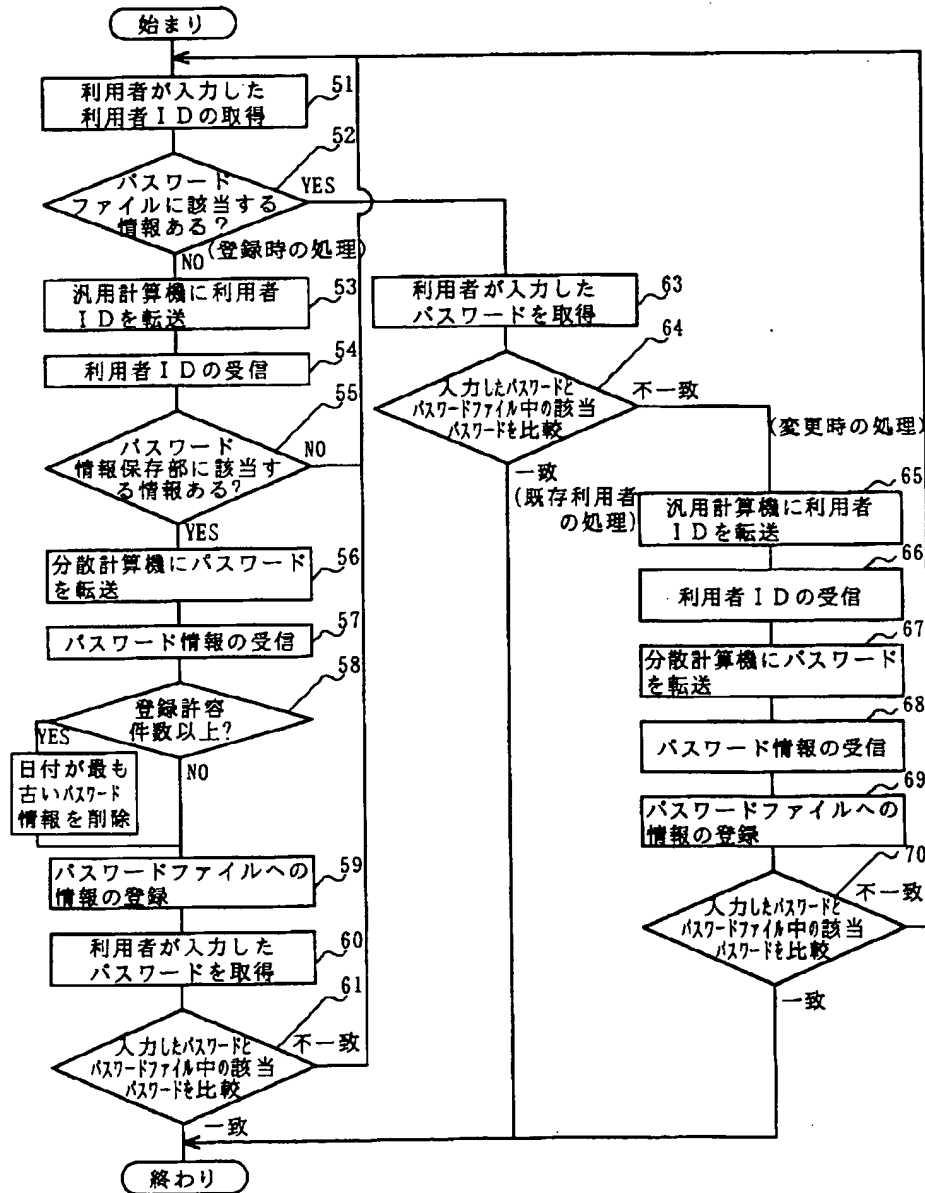
【図 9】

図 9

USERM	PWDZ	93.09.03
USERK	PWDK	93.09.02
USERJ	PWDJ	93.07.21
USERI	PWDI	93.08.29
USERH	PWDH	93.07.21

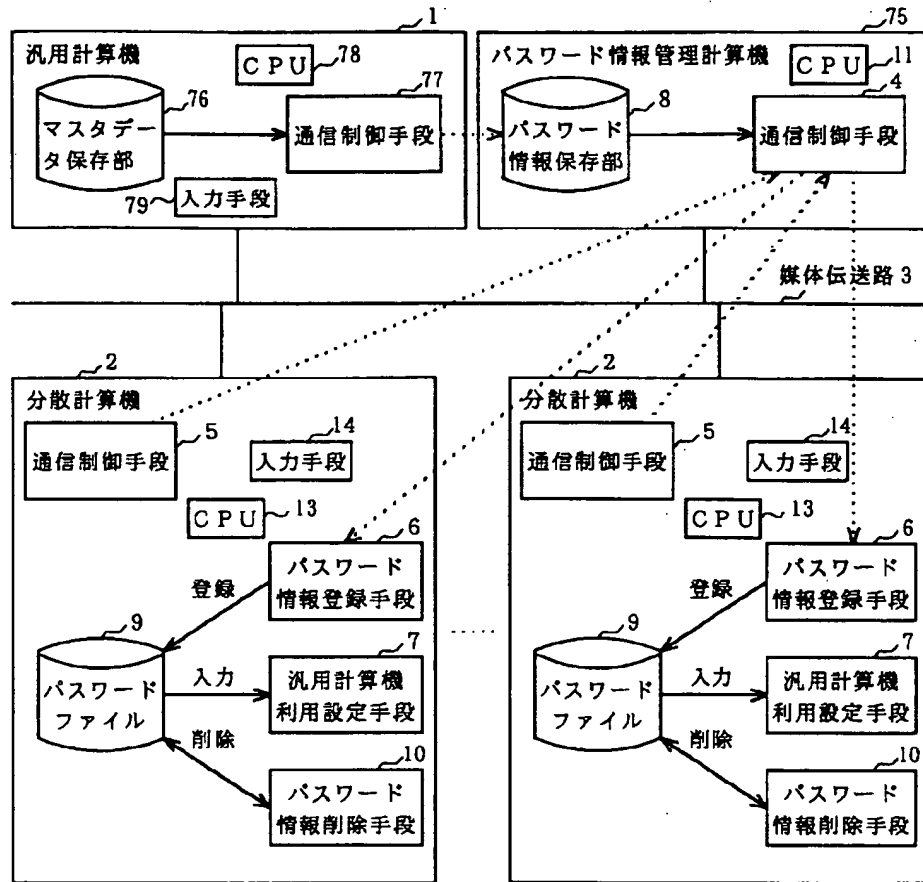
【図 10】

図 10



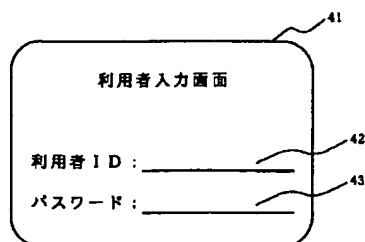
【図 1 1】

図 1 1



【図 1 2】

図 1 2



## フロントページの続き

- (72)発明者 森 正則  
神奈川県川崎市幸区鹿島田890番地の12  
株式会社日立製作所情報システム事業部内
- (72)発明者 森 利幸  
神奈川県川崎市幸区鹿島田890番地の12  
株式会社日立製作所情報システム事業部内
- (72)発明者 佐藤 一尋  
神奈川県川崎市幸区鹿島田890番地の12  
株式会社日立製作所情報システム事業部内
- (72)発明者 増田 隆宏  
神奈川県横浜市中区尾上町 6 丁目81番地  
日立ソフトウェアエンジニアリング株式会  
社内